# Aruba Instant Access Point Configuration Guide

This guide assumes that you already have a working open WLAN.

## Upload Certificate

You must upload your own certificate to the Aruba IAP. Without doing this, the default Aruba certificate will be used which will cause security warnings for most users, and may even prevent them from connecting to the captive portal. Please ensure you have your certificate signed by a certificate authority, as using a self-signed certificate will also cause security warnings for users trying to connect. Ensure your certificate is in PEM format and contains keys/certificates in the following order: **private key, certificate, CA certificate, CA intermediate certificates, CA root certificate.** For more information, see http://community.arubanetworks.com/t5/Controller-Based-WLANs/ArubaOS-Default-Certificate-Revocation-FAQ-Controllers/ta-p/275809.

Step 1 Click **Maintenance**.

Step 2 Open the **Certificates tab**.

Step 3 Choose the **certificate file** you want to upload.

Step 4 Choose **Auth for Certificate Type**.

Step 5 Choose your certificate format.

Step 6 Click **Upload Certificate**.

Step 7 Repeat steps 3-6, but use **Captive Portal Server** for **Certificate Type**.

Note that the AP may reboot automatically after uploading one or both of these **certificates**. To verify that the certificates have been uploaded properly, in the Certificates tab, you should see an entry for **Current Server Certificate** and for **Current CP Server Certificate.** Take note of the Common Name of the certificate by checking the value after **CN=** in the **Subject** field.

## Configure Authentication

Navigate to **Security.** All authentication configuration will take place on this page.

**Add RADIUS Servers**

Step 1 Open the **Authentication Servers** tab.

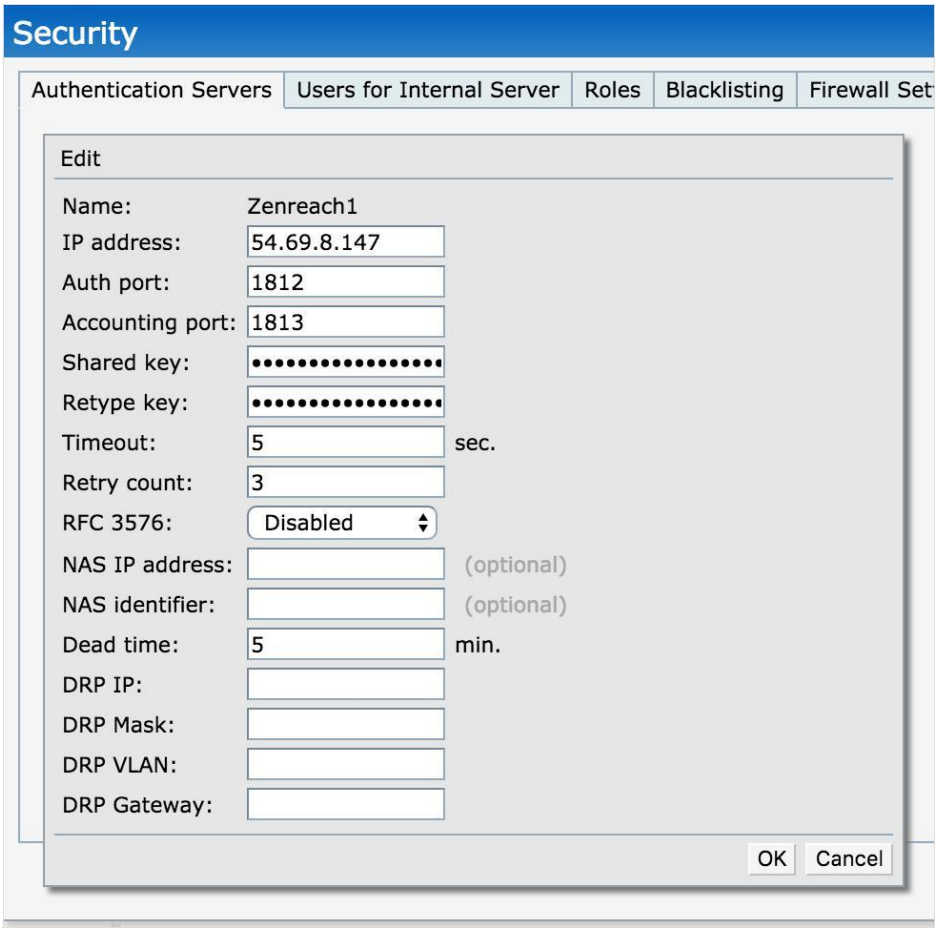
Step 2 Click **New**.

Step 3 Select the **RADIUS** option.

Step 4 Enter the settings from the table below into the form.

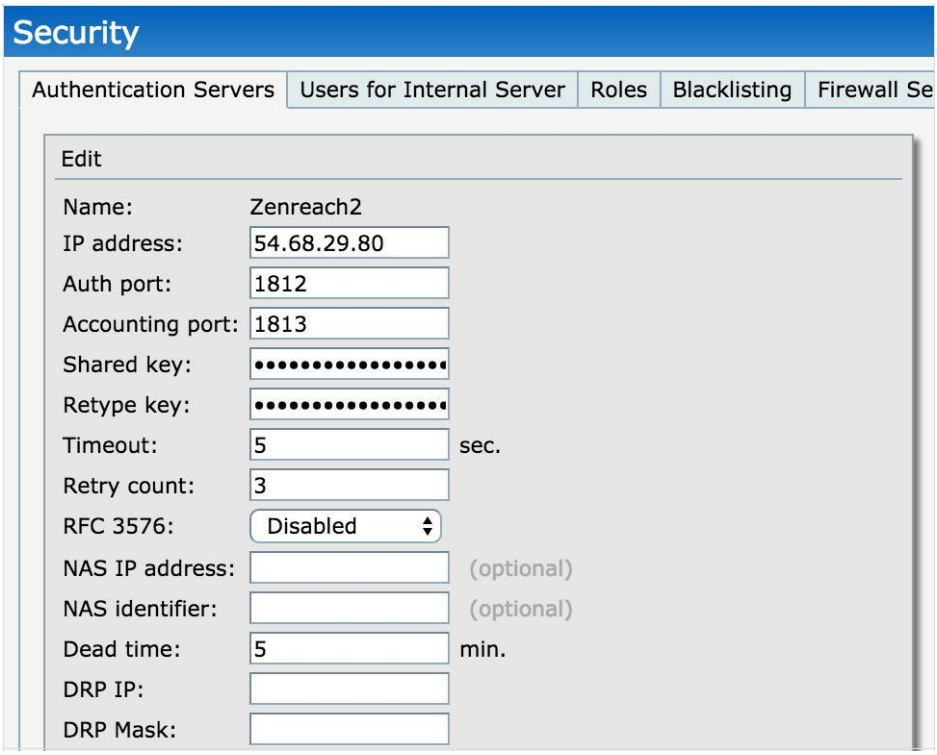
Step 5 Click **OK** when finished.

**Name:** Zenreach1
**IP address:** 54.69.8.147
**Auth port:** 1812
**Accounting port:** 1813
**Timeout:** 5
**Retry count:** 3
**Shared key:** 8fc40973252c42e196489d4a16849ff8
**Retype key:** 8fc40973252c42e196489d4a16849ff8



Repeat steps 2-5 to add a second server using the following settings:

**Name:** Zenreach2
**IP address:** 54.68.29.80
**Auth port:** 1812
**Accounting port:** 1813
**Timeout:** 5
**Retry count:** 3
**Shared key:** 8fc40973252c42e196489d4a16849ff8
**Retype key:** 8fc40973252c42e196489d4a16849ff8




**Add Captive Portal Authentication**

A captive portal authentication profile must now be created.

Step 1 Open the **External Captive Portal** tab.

Step 2 Click **New**.

Step 3 Enter the settings from the table below into the form.

Step 4 For the URL setting, replace **AP_MAC_ADDRESS_HERE** with the MAC address of any one of the APs in your network. The format of the MAC address **must** be lowercase and colon delimited.
eg. **ab:12:cd:34:ef:56**

Step 5 Also in the URL setting, replace **CERTIFICATE_CN_HERE** with the Common Name in the certificate you added in the **Upload Certificate** section of this document. If you are using a wildcard certificate (eg. *.mycompany.com), then you must replace the asterisk (*) with **captiveportal-login**, making it **captiveportal-login.mycompany.com**.

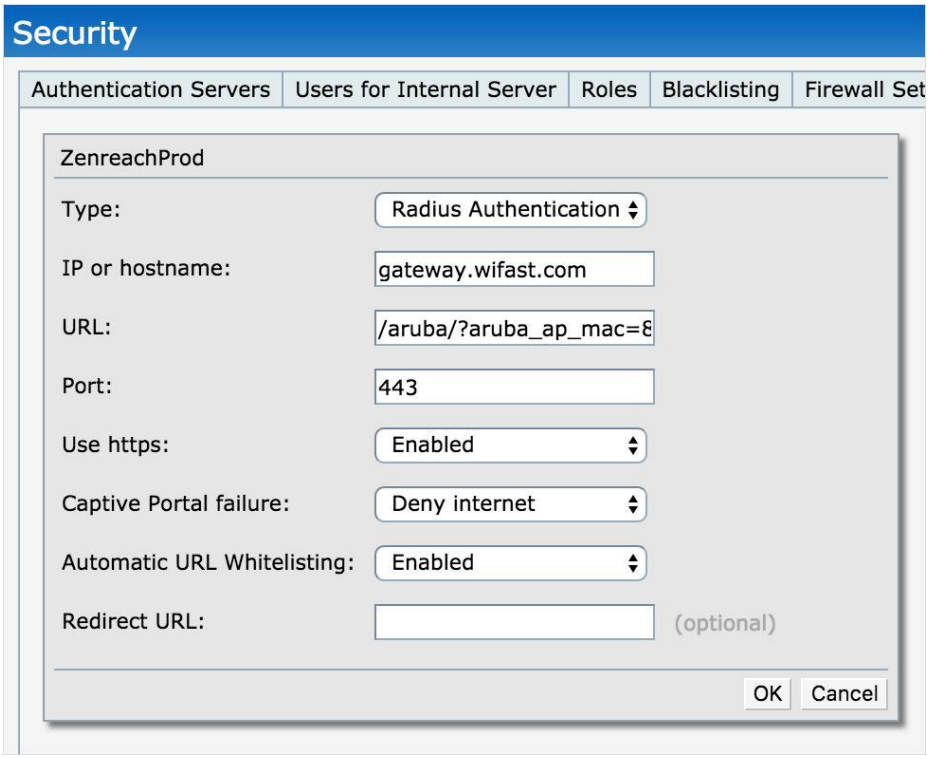
Step 6 Click **OK.**

**Name:** Zenreach
**Type:** Radius Authentication
**IP or hostname:** gateway.wifast.com

**URL:** /aruba/?aruba_ap_mac=AP_MAC_ADDRESS_HERE&auth_url=CERTIFICATE_CN_HERE

**Port:** 443
**Use http:** Enabled
**Captive Portal failure:** Deny internet
**Automatic URL Whitelisting:** Enabled
**Redirect URL:** Make sure this is blank

(NOTE: You MUST replace AP_MAC_ADDRESS_HERE with any of your AP MAC addresses and CERTIFICATE_CN_HERE with the CN from your certificate as noted in the steps above)




Click **OK** to exit the **Security** page.

## AP Configuration

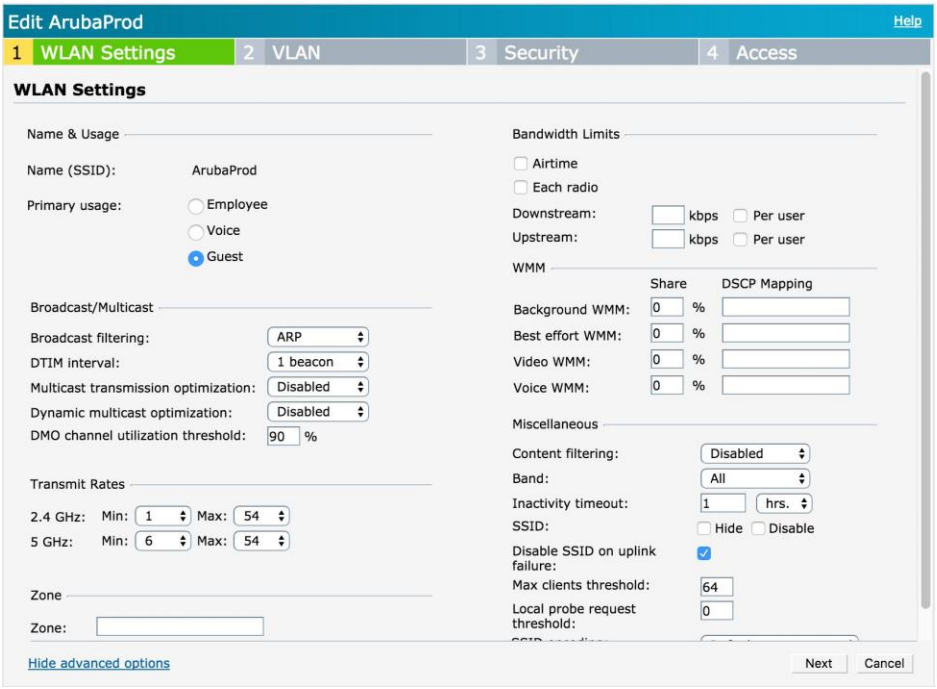
Step 1 Select the AP under **Networks** section.

Step 2 Click **Edit**.

Step 3 In the **WLAN Settings** step, choose the **Guest** option for **Primary usage**.

Step 4 Click **Show Advanced Options**.

Step 5 Set **Inactivity Timeout to 1 hrs.**




Step 7 Click **Next.**

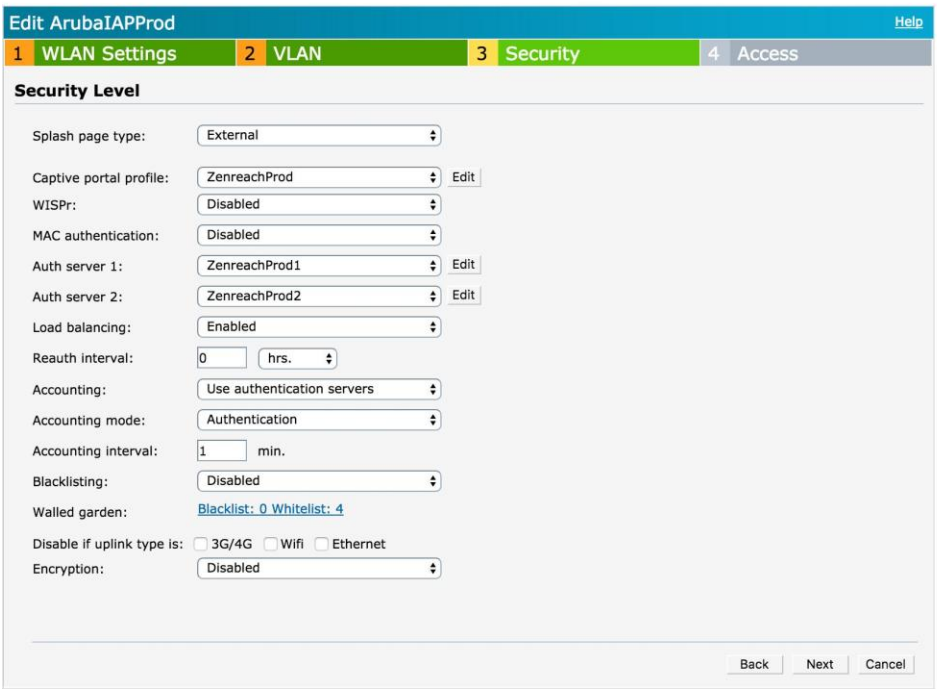
Step 8 Click **Next** to go to the **Security** step.

Step 9 Enter the settings from the table below into the form.

Step 10 Click **Next.**

Step 11 Click **Finish.**

**Splash page type:** External
**Captive portal profile:** Zenreach
**Auth server 1:** Zenreach1
**Auth server 2:** Zenreach2
**Load balancing:** Enabled
**Accounting:** Use authentication servers
**Accounting mode:** Authentication
**Accounting interval:** 1 min




## Configure Location Services

Step 1 Click **More**, then **Services**.

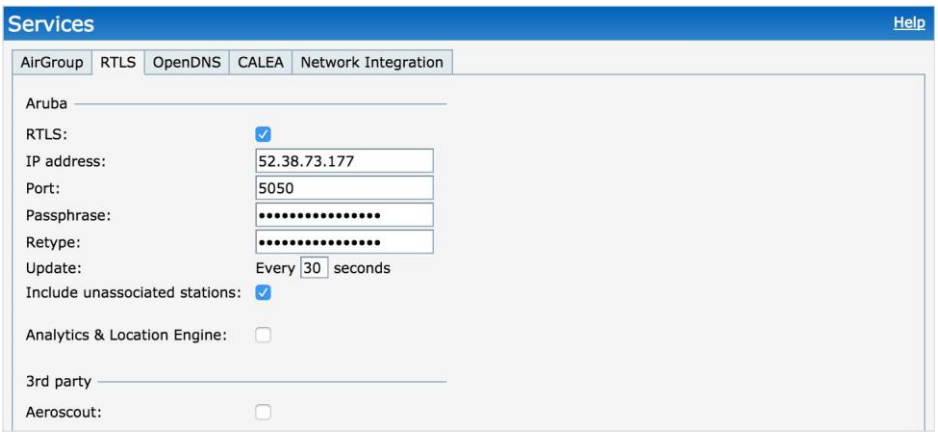
Step 2 Open the **RTLS** tab.

Step 3 Check the **RTLS** checkbox.

Step 4 Fill in the form with the information below.

Step 5 Click **OK**.

**IP address:** 52.38.73.177
**Port:** 5050
**Passphrase:** Laepael9lu1iique
**Retype:** Laepael9lu1iique
**Update:** 30
**Include unassociated stations:** Checked



# Walled Garden for Social Login

A walled garden is a list of websites whitelisted for access before the user is authenticated. Prior to enabling the Social Login feature, the walled garden will need to be configured for each of the respective social network.

### Facebook and Twitter

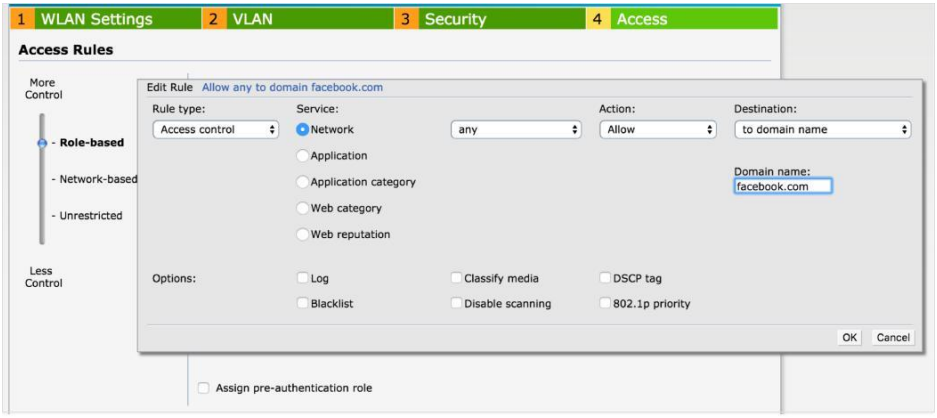
Step 1 **Enable Automatic URL Whitelisting** in the **External Captive Portal profile.**

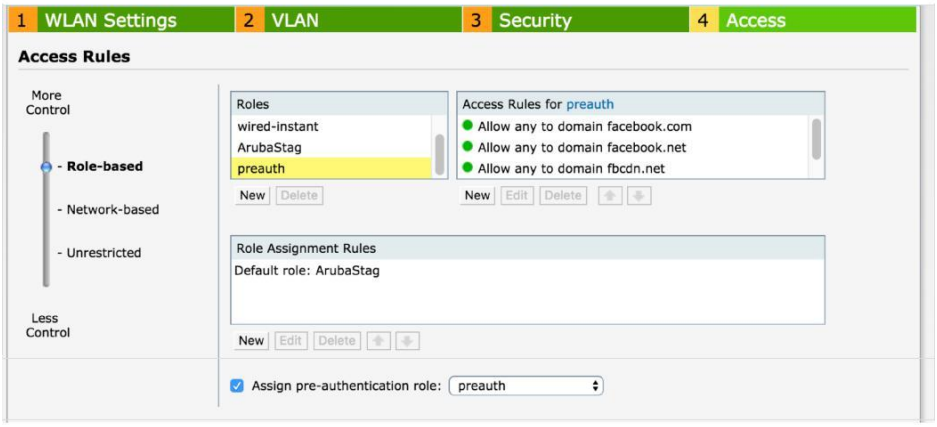
Step 2 Go to **Security**, then **Walled Garden** tab.

Step 3 Add the facebook and twitter domains to the Walled Garden whitelist.

facebook.com
facebook.net
fbcdn.net
akamaihd.net
twitter.com
twimg.com

Step 4 Edit your network configuration, and go to the **Access** tab. Create a role for pre-authentication called **preauth** and add ACL rules for each of the above domains. Check the Assign **pre-authentication role** box and select **preauth**.






For questions or comments about this integration guide,
please contact partners@zenreach.com.